United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Committee on Science, House of Representatives

For Release on Delivery
Expected at
10 a.m.
Wednesday,
May 10, 2000

INFORMATION SECURITY

"ILOVEYOU" Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements

Statement of Keith A. Rhodes
Director, Office of Computer and Information Technology Assessment
Accounting and Information Management Division

G A O
Accountability * Integrity * Reliability

GAO/T-AIMD-00-171

Madam Chairwoman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on the "ILOVEYOU" computer virus. About this time last year, I testified before this Subcommittee on the "Melissa" virus, which temporarily disrupted the operations of some agencies by forcing them to shut down their e-mail systems.[1] At that hearing, I stressed that the next virus would likely propagate faster, do more damage, and be more difficult to detect and counter. This is just what we have experienced with ILOVEYOU. While it looked a lot like Melissa in its operation, it moved much more swiftly, and it appears to have caused as much, if not more, disruption.

Nevertheless, the lessons to be gleaned from both attacks are the same. Federal agencies must implement vigorous security programs to enable them to closely watch their information resources for signs of attack or intrusion and to quickly react to such events when detected. Moreover, the government as a whole must promptly implement long-term solutions that will ensure that agencies focus on security from an organizationwide perspective and implement a comprehensive set of security controls. It must also establish central tracking and reporting mechanisms to facilitate analyses of these and other forms of attacks and their impact.

The ILOVEYOU Worm/Virus and Its Immediate Impact

ILOVEYOU is both a "virus" and "worm." Worms propagate themselves through networks; viruses destroy files and replicate themselves by manipulating files. The damage resulting from this particular hybrid—which includes overwhelmed e-mail systems and lost files–is limited to users of the Microsoft Windows operating system.

ILOVEYOU typically comes in the form of an e-mail message from someone the recipient knows with an attachment called LOVE-LETTER-FOR-YOU.TXT.VBS. The attachment is a Visual Basic Script (VBS) file.[2] As long as recipients do not run the attached file, their systems will not be affected and they need only to delete the e-mail and its attachment. When opened and allowed to run, however, ILOVEYOU attempts to

[1] *Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data* (GAO/T-AIMD-99-146, April 15, 1999).

[2] VBS is a subset of Microsoft's Visual Basic program language intended for use in World Wide Web browsers and certain other applications.

- send copies of itself using Microsoft Outlook (an electronic mail software program) to all entries in all of the recipient's address books,
- infect the Internet Relay Chat (IRC) program[3] so that the next time a user starts "chatting" on the Internet, the worm can spread to everyone who connects to the chat server,
- search for picture, video, and music files and overwrite or replace them with a copy of itself, and
- install a password-stealing program that will become active when the recipient opens Internet Explorer[4] and reboots the computer. (Internet accounts set up to collect this information were reportedly disabled early Friday).

In short, ILOVEYOU looks a lot like Melissa in operation: it comes via e-mail; it attacks Microsoft's Outlook; it's a hybrid between a worm and a virus; and it does some damage–but it mostly excels at using the infected system to e-mail copies of itself to others. The one main difference is that it proliferated much faster than Melissa because it came during the work week, not the weekend. Moreover, ILOVEYOU sent itself to everyone on the recipient's e-mail lists, rather than just the first 50 addressees as Melissa did.

In fact, soon after initial reports of the worm/virus surfaced in Asia on May 4, ILOVEYOU spread rapidly throughout the rest of the world. By 6 pm the same day, Carnegie Mellon's CERT Coordination Center[5] had received over 400 direct reports involving more than 420,000 Internet hosts. And by the next day, ILOVEYOU appeared in new guises, labeled as "Mother's Day," "Joke," "Very Funny," among others. At least 14 different variants of the virus had been identified by the weekend, according to DOD's Joint Task Force-Computer Network Defense. These variations retriggered disruptions because they allowed the

[3]A program that enables people connected anywhere on the Internet to join in live discussions. Unlike older chat systems, IRC is not limited to just two participants. The IRC client sends the participant's messages to and receives messages from an IRC server. The IRC server is responsible for making sure that all messages are broadcast to everyone participating in a discussion.

[4]Microsoft's World Wide Web browser.

[5]Originally called the Computer Emergency Response Team, the center was established in 1988 by the Defense Advanced Research Projects Agency. It is charged with establishing a capability to quickly and effectively coordinate communication among experts in order to limit the damage associated with and respond to incidents and to build awareness of security issues across the Internet community.

worm/virus to bypass filters set up earlier to block ILOVEYOU. At least one variant—with the subject header "VIRUS ALERT!!!"–was reportedly even more dangerous than the original because it was also able to overwrite system files critical to computing functions.

Reports from various media, government agencies, and computer security experts indicate that the impact of ILOVEYOU was extensive. The virus reportedly hit large corporations such as AT&T, TWA, and Ford Motor Company; media outlets such as the Washington Post and ABC news; international organizations such as the International Monetary Fund, the British Parliament, and Belgium's banking system; state governments; school systems; and credit unions, among many others, forcing them to take their networks off-line for hours.

The virus/worm also reportedly penetrated at least 14 federal agencies—including the Department of Defense (DOD), the Social Security Administration, the Central Intelligence Agency, the Immigration and Naturalization Service, the Department of Energy, the Department of Agriculture, the Department of Education, the National Aeronautics and Space Administration (NASA), along with the House and Senate. We still do not know the full effect of this virus on the agencies that were penetrated. While many were forced to shut down their e-mail networks for some time, many also reported that mission-critical systems and operations were not affected. Of course, if an agency's business depends on e-mail for decision-making and service delivery, then the virus/worm probably had a significant impact on day-to-day operations in terms of lost productivity.

It also appears that major efforts were required to control the virus. Based on a discussion with military CERT representatives, for example, responding to the virus/worm has been a tremendous task that took several days to get under control. Some DOD machines required complete software reloads to overcome the extent of the damage. The virus/worm spread rapidly through the department, penetrating even some classified systems. DOD's operational commands responded in widely varying ways—some made few changes to their daily operational procedures while others cut off all e-mail communications for an extended period of time. Representatives of DOD's Joint Task Force-Computer Network Defense said that they will recommend new procedures to better coordinate the department's response to future incidents, based on experience with the ILOVEYOU virus/worm.

Virus/Worm Reiterates Challenge in Protecting Information Technology Assets and Sensitive Data

While the ILOVEYOU worm/virus resulted in relatively limited damage in terms of systems corrupted, the incident continues to underscore the formidable challenge that the federal government faces in protecting its information systems assets and sensitive data. It again shows, for example, that computer attack tools and techniques are becoming increasingly sophisticated; viruses are spreading faster as a result of the increasing connectivity of today's networks; commercial-off-the-shelf (COTS) products can be easily exploited for attack by all their users; and there is no "silver bullet" solution to protecting systems, such as firewalls or encryption.

Moreover, ILOVEYOU illustrates the difficulty of investigating cyber crime. In particular, investigations of computer attacks such as ILOVEYOU must be conducted on an international scale. Moreover, only the computer used to launch the virus can be traced–not the programmer. Lastly, evidence is fleeting–the more time that passes between the first attack and an arrest, the more time the programmer has to destroy all links to the crime.

Additionally, ILOVEYOU once again proved that governmentwide reporting mechanisms are ineffective. Like Melissa more than a year ago, little information was available early enough for agencies to take proactive steps to mitigate the damage. The CERT Coordination Center posted its advisory at approximately 9:30 pm May 4, while FBI's National Infrastructure Protection Center (NIPC) issued a brief notice at 11:00 am on May 4 and more information at 10:00 pm. In addition, there is still no complete information readily available on the impact that this virus had across the federal government.

More important, like Melissa and other attacks this Subcommittee has focused on, our experience with ILOVEYOU is a symptom of broader information security concerns across government. Over the past several years, our analyses as well as those of the inspectors general have found that virtually all of the largest federal agencies have significant computer security weaknesses that place critical federal operations and assets at risk to computer-based attacks. Our most recent individual agency review, of the Environmental Protection Agency (EPA),[6] identified many security weaknesses associated with the computer operating systems and the agencywide computer network that support most of EPA's mission-related and financial operations. In addition,

[6] *Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk* (GAO/T-AIMD-00-97, February 17, 2000).

EPA's own records identified serious computer incidents in the last 2 years. EPA is currently taking significant steps to address these weaknesses, but resolving them on a lasting basis will require substantial ongoing management attention and changes in the way EPA views information security.

EPA is not unique. Within the past 12 months, we have identified significant management weaknesses and control deficiencies at a number of agencies, including DOD, NASA, State, and VA. Although the nature of operations and related risks at these and other agencies vary, there are striking similarities in the specific types of weaknesses reported. I would like to briefly highlight six areas of management and general control problems since they are integral to understanding and implementing long-term solutions.

- First, we continue to find that poor security planning and management is the rule rather than the exception. Most agencies do not develop security plans for major systems based on risk, have not formally documented security policies, and have not implemented programs for testing and evaluating the effectiveness of controls they rely on. These are fundamental activities that allow an organization to manage its information security risks cost-effectively rather than by reacting to individual problems ad hoc.

- Second, agencies often lack effective access controls to their computer resources (data, equipment, and facilities) and, as a result, are unable to protect these assets against unauthorized modification, loss, and disclosure. These controls would normally include physical protections such as gates and guards and logical controls, which are controls built into software that (1) require users to authenticate themselves through passwords or other identifiers and (2) limit the files and other resources that an authenticated user can access and the actions that he or she can take.

- Third, in many of our audits we find that application software development and change controls are weak. For example, testing procedures are undisciplined and do not ensure that implemented software operates as intended, and access to software program libraries is inadequately controlled.

- Fourth, many agencies lack effective policies and procedures governing the segregation of duties. We commonly find that computer programmers and operators are authorized to perform a wide variety of duties, such as independently writing, testing, and approving program

changes. This, in turn, provides them with the ability to independently modify, circumvent, and disable system security features.

- Fifth, our reviews frequently identify systems with insufficiently restricted access to the powerful programs and sensitive files associated with the computer system's operation, e.g., operating systems, system utilities, security software, and database management system. Such free access makes it possible for knowledgeable individuals to disable or circumvent controls.
- Sixth, we have found that service continuity controls are incomplete and often not fully tested for ensuring that critical operations can continue when unexpected events (such as a temporary power failure, accidental loss of files, major disaster such as a fire, or malicious disruptions) occur.

Actions Needed to Prepare for Future Computer Attacks

Agencies can act immediately to address the weaknesses I just described and thereby reduce their vulnerability to computer attacks, including the ILOVEYOU worm/virus. Specifically, as explained in figure 1, they can (1) increase awareness, (2) ensure that existing controls are operating effectively, (3) ensure that software patches are up-to-date, (4) use automated scanning and testing tools to quickly identify problems, (5) expand their best practices, and (6) ensure that their most common vulnerabilities are addressed.

Figure 1: Actions Agencies Can Take To Immediately Reduce Risks

☐ ***Ensure that agency personnel at all levels understand the significance of their dependence on computer support and the related risks to mission-related operations.***	Better understanding of risks allows senior executives to make more informed decisions regarding appropriate levels of financial and personnel resources to protect these assets over the long term.
☐ ***Ensure that policies and controls already implemented are operating as intended.***	Our audits often find that security is weak, not because agencies have no policies and controls, but because the policies and controls they have implemented are not operating effectively.
☐ ***Ensure that known software vulnerabilities are reduced by promptly implementing software patches.***	Security weaknesses are frequently discovered in commercial software packages after the software has been sold and implemented. To remedy these problems, vendors issue software "patches" that users can install. In addition, organizations such as the CERT Coordination Center routinely issue alerts on software problems.
☐ ***Use readily available software tools to help ensure that controls are operating as intended and that systems are secure.***	Examples of such tools are (1) scanners that automatically search for system vulnerabilities, (2) password cracking tools, which test password strength, and (3) network monitoring tools, which can be used to monitor system configuration and network traffic, help identify unauthorized changes, and identify unusual or suspicious network activity.
☐ ***Expand on the good practices that are already in place in the agency.***	Our audits have shown that even agencies with poor security programs often have good practices in certain areas of their security programs or certain organizational units. In these cases, we recommend that the agency expand or build on these practices throughout the agency.
☐ ***Develop and distribute lists of the most common types of vulnerabilities, accompanied by suggested corrective actions.***	Such lists enable individual organization units to take advantage of experience gained by others. They can be developed based on in-house experience, or adapted from lists available through professional organizations and other centers of expertise.

To combat viruses and worms specifically, agencies could take steps such as ensuring that security personnel are adequately trained to

respond to early warnings of attacks and keeping antivirus programs up-to-date. Strengthening intrusion detection capabilities may also help. Clearly, it is difficult to sniff out a single virus attached to an e-mail coming in but if 100 e-mails with the same configuration suddenly arrive, an alert should be sounded. User education is also key. In particular, agencies can teach computer users that e-mail attachments are not always what they seem and that they should be careful when opening them. By no means, should users open attachments whose filenames end in ".exe" unless they are sure they know what they are doing. Users should also know that they should never start a personal computer with an unscanned floppy disk or CD-ROM in the computer drive.

I would like to stress, however, that while these actions can jump-start security improvement efforts, they will not result in fully effective and lasting improvements unless they are supported by a strong management framework. Based on our 1998 study[7] of organizations with superior security programs, this involves managing information security risks through a cycle of risk management activities that include

- assessing risks and determining protection needs,
- selecting and implementing cost-effective policies and controls to meet these needs,
- promoting awareness of policies and controls, and of the risks that prompted their adoption, among those responsible for complying with them, and
- implementing a program of routine tests and examinations for evaluating the effectiveness of policies and related controls and for reporting the resulting conclusions to those who can take appropriate corrective action.

Additionally, a strong central focal point can help ensure that the major elements of the risk management cycle are carried out and can serve as a communications link among organizational units. Such coordination is especially important in today's highly networked computer environment.

[7] *Executive Guide: Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998).

I would also like to emphasize that while individual agencies bear primary responsibility for the information security associated with their own operations and assets, there are several areas where governmentwide criteria and requirements also need to be strengthened. First, there is a need for routine periodic independent audits of agencies to provide (1) a basis for measuring agency performance and (2) information for strengthened oversight. Except for security audits associated with financial statement audits, current information security reviews are performed on an ad hoc basis.

Second, agencies need more prescriptive guidance regarding the level of protection that is appropriate for their systems. Currently, guidance provided by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) allows agencies wide discretion in deciding what computer security controls to implement and the level of rigor with which they enforce these controls. As a result, existing guidance does not ensure that agencies are making appropriate judgments in this area and that they are protecting the same types of data consistently throughout the federal community. More specific guidance could be developed in two parts: the first being a set of data classifications that could be used by all federal agencies to categorize the criticality and sensitivity of the data they generate and maintain and the second being a set of minimum mandatory control requirements for each classification which would cover such issues as the strength of system user authentication techniques, appropriate types of cryptographic tools, and the frequency and rigor of testing.

Third, there is a need for stronger central leadership and coordination of information security related activities across government. Under current law, responsibilities for guidance and oversight of agency information security is divided among a number of agencies, including OMB, NIST, the General Services Administration, and the National Security Agency. Other organizations have become involved through the administration's critical infrastructure protection initiative, including the FBI's National Infrastructure Protection Center and the Critical Infrastructure Assurance Office. The federal Chief Information Officers Council is also supporting these efforts. While all of these organizations have made positive contributions, some roles and responsibilities are not clear, and central coordination is lacking in key areas. In particular, as this latest attack showed, information on vulnerabilities and related solutions is not being adequately shared among agencies, and requirements related to handling and reporting security incidents are not clear.

In conclusion, more than 12 months later, not much is different with the ILOVEYOU worm/virus than with Melissa. Many agencies were hit; most were fortunate that the worst damage done was to shut down e-mail systems and temporarily disrupt operations; and early warning systems for incidents like these still need to be improved. Moreover, our audits continue to find that most agencies continue to lack the basic management framework needed to effectively detect, protect against, and recover from these attacks. Lastly, as seen with ILOVEYOU's variations, we can still expect the next virus to propagate faster, do more damage, and be more difficult to encounter. Consequently, it is more critical than ever that federal agencies and the government act as whole to swiftly implement both short- and long-term solutions identified today to protect systems and sensitive data.

Madam Chairwoman, this concludes my testimony. I would be happy to answer any questions you or Members of the Subcommittee may have.

Contacts and Acknowledgments

For information about this testimony, please contact Keith Rhodes at (202) 512-6415. Cristina Chaplain made key contributions to this testimony.

(511998)

Ordering Information

Orders by Internet

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

Web site: http://www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

1-800-424-5454 (automated answering system)